DOI: 10.37791/2687-0649-2021-16-4-96-109

Virtualization of information object vulnerability testing container based on DeX technology and deep learning neural networks

B. Okunev[1]***, A. Lazarev***[1*]***, P. Kharlamov***[1]
[1] *Branch of the National Research University "MPEI" in Smolensk, Smolensk, Russia*
** anonymous.prodject@gmail.com*

Abstract. The modern development of information security tools, along with the improvement of remote access methods, allows software and hardware to be audited without the need for direct access to the system under test. One of its components is related to the implementation of software on mobile ARM processor architectures. Within this direction of development, the approach that allows integrating Linux kernel-based distributions by introducing a virtual container chroot (change root) into the Android OS-based system and, consequently, performing penetration testing without the need to use personal computers is highlighted. An example of this approach is the Kali NetHunter distribution which allows remote system administration functionality through the KeX module. Besides the obvious advantages of KeX functionality, some disadvantages should also be mentioned: firstly, the low speed of GUI processing due to translation to remote hosts and the need to support translation at operating system level; secondly, the consumption of energy resources when using the desktop features of the KeX module. In order to solve the mentioned problems, a system of virtualization of energy-efficient container for testing the vulnerabilities of critical information objects has been developed and based on the principle of multi-containerization. The software of the system is represented by two components: an enlarged module for integration of the chroot container into the DeX environment (primary), and an enlarged module for ensuring energy efficiency using predictive neural network models based on variable time intervals (secondary). As a result of comparing the effectiveness of existing and implemented approaches in penetration testing, it is noted that the proposed system can be used in testing the security of particular platforms and systems, including highly sensitive information objects or resources.

Keywords: information security, deep learning neural networks, data virtualization, penetration testing

For citation: Okunev B., Lazarev A., Kharlamov P. Virtualization of information object vulnerability testing container based on DeX technology and deep learning neural networks. *Prikladnaya informatika*=Journal of Applied Informatics, 2021, vol.16, no.4, pp.96-109. DOI: 10.37791/2687-0649-2021-16-4-96-109

Виртуализация контейнера тестирования уязвимостей информационных объектов на основе технологии DeX и нейронных сетей глубокого обучения

Б. В. Окунев[1]***, А. И. Лазарев***[1*]***, П. С. Харламов***[1]
[1] *Филиал ФГБОУ ВО «Национальный исследовательский университет "МЭИ"» в г. Смоленске, Смоленск, Россия*
** anonymous.prodject@gmail.com*

Аннотация. Современное развитие средств обеспечения информационной безопасности, наряду с усовершенствованием методик удаленного доступа, позволяет производить аудит программно-аппаратных компонентов без необходимости прямого доступа к тестируемой системе. В рамках данного направления развития выделяется подход, позволяющий интегрировать дистрибутивы на базе ядра Linux представлением виртуального контейнера chroot в системе на базе Android OS и, как следствие, осуществлять тестирование на проникновение без необходимости использования персональных компьютеров. Примером реализации данного подхода является дистрибутив Kali NetHunter, позволяющий за счет модуля KeX реализовать функционал удаленного администрирования системой. Кроме очевидных преимуществ KeX функционала также следует выделить ряд недостатков – низкая скорость обработки графической оболочки за счет трансляции на удаленных хост и необходимость поддержки трансляции на уровне операционной системы. Вторая проблема – затраты энергоресурсов при использовании возможностей рабочего стола в KeX модуле. Для решения указанных проблем была разработана система виртуализации энергоэффективного контейнера тестирования уязвимостей критически важных информационных объектов, основной принцип действия которой – мульти-контейнеризация. Программная составляющая представлена двумя элементами: модулем интеграции контейнера chroot в среду DeX и модулем обеспечения энергоэффективности за счет использования предиктивных моделей нейронных сетей. В результате сравнения эффективности существующих и реализованного подхода при тестировании на проникновение отмечено, что предлагаемая система может быть использована при тестировании безопасности различных информационных объектов.

Ключевые слова: информационная безопасность, нейронные сети глубокого обучения, виртуализация данных, тестирование на проникновение

Для цитирования: *Окунев Б. В., Лазарев А. И., Харламов П. С.* Virtualization of information object vulnerability testing container based on DeX technology and deep learning neural networks // Прикладная информатика. 2021. Т. 16. № 4. С. 96–109. DOI: 10.37791/2687-0649-2021-16-4-96-109

Introduction

The investigation of processes for the purpose of evaluating information security is generally represented by testing the hardware and software of the target device. Nowadays there are various distributions for testing based on the Linux kernel, which include a list of popular attack tools in variant vectors [1]. Examples of such systems are the Kali Linux distribution from Offensive